**Notes from VWV Academies Annual Update (also useful for maintained schools)**

**June 2017**

**KCSIE - reminders**

1. Governors and directors are required to ensure that there are mechanisms in place to help staff understand and discharge their roles and responsibilities with regard to KCSIE. (para 45)
2. Governors and directors must ensure that the CP policy minimises risk of peer on peer abuse and states how such allegations will be dealt with. (paras 47, 48, 76)
3. Governors and Directors must recognise that there may be additional barriers for children with SEN. (paras 51, 85)
4. Staff know-how must be fed into the KCSIE policy so that it reflects the individual school. ( Annex B. para 66)
5. Chairs need to have more training on dealing with allegations. (para 73, 74, 151)
6. There must be clear protocols for sending records to the next school and each school must take account of local protocols as information dissemination as required by the LSCB.
7. There must be a MAT director checking safeguarding across the Trust. They are to be the point of contact for the DSL’s. Directors must have training and also have liability insurance. (paras 46, 52, 81)
8. All staff should have regular emails and bulletins keeping them up to date on CP. (paras 13, 68, 72)
9. Computers should have appropriate filters but there must not be over-blocking. (paras 67, 69 and Annex C)
10. From Sept 16 there were new regulations regarding registers. In addition to informing the LA when a name is going to be deleted schools must now inform within 5 days when a name is added. Schools must also inform the LA when a pupil has been absent for more than 10 consecutive school days.
11. Failing to protect a girl from FGM is now a criminal offence and reporting is mandatory.
12. Sexting must be included in the CP policy.
13. Schools should have access to the new Prevent resources launched in 2016. [www.educateagainsthate.com](http://www.educateagainsthate.com) and https//elearning.prevent.homeoffice.gov.uk/
14. There is a consultation going on about disqualification by association and there seems to be some emphasis on pre and post school clubs.

**Term Time Holidays June 2017**

The issue has been live since the case brought in the Isle of Wight about what the Law means by ‘attend regularly’. (Ed Act 1996 sect 444). The LA lost and appealed the case.

The Supreme Court decided that it means ‘**In accordance with the rules’**.

This means any failure to attend regularly can result in prosecution although Head’s may give permission to be absent in **exceptional** cases.

A failure could include:

* A single of half day unauthorised absence
* Arriving after the register is closed
* Leaving early without authorisation
* Any other failure in accordance with the rules.

This means that LA’s will have to review codes of Conduct. Consider fixed penalties and establish exactly what constitutes technical and minor breaches.

Schools will have to:

* review existing policies and procedures
* remind parents about the rules
* record and monitor carefully requests for leave and action taken
* be ready for the new DfE guidance which is almost certain to appear.

**Exclusions June 2017**

Make sure you are using DfE guidance 2012. Do **not** use Google to find it as it brings up the wrong information.

New guidance is on the way which will provide:

* More clarity for governors and independent review panels
* Updates on the requirement to arrange education for the pupil form the 6th day
* Changes with regard to pupils with SEN and EHCP’s
* Non-statutory guidance for Heads
* QA for parents

Changes will include:

* Exclusions cannot be extended of converted
* Consecutive fixed period exclusions are considered cumulative
* A definition of ‘proof’
* Defining a Head’s duty regarding notification of parents
* Defining a Governing body’s responsibilities for the pupil
* Academy Trust’s responsibilities defined
* Role of the SEN expert
* Notifications that must be made
* The governing body’s duty to consider reinstatement

This will mean:

* Behaviour and discipline procedures and policies need to be revised
* Training for Head’s governors and IRP’s
* Ensuring there are resources available for admin costs and personnel
* Communication changes to parents

Due to be published this summer to take effect from September 1st  2017.

**The General Data Protection Regulation (GDPR) June 2017**

Previous regulation was via Data Protection Act which is now 20 years old.

It will apply from 25th May 2018.

GDPR :

* Much more prescriptive
* Emphasis on security
* Transparency is a key theme
* Keeping a record of compliance
* Individuals rights spelt out

Schools are **required** to comply with 8 data protection principles.

Individuals have rights e.g. to make subject access requests

The maximum fine is the higher of £20 million or 4% of turnover. (it is currently half a million).

To make a claim you no longer have to prove financial loss – it could just be stress e.g. a case was won over using a child’s photograph.

Security

This has been the source of most fines

To keep data secure there must already be:

* Network security, firewalls, anti-virus
* Policies, procedures
* Training
* Audits and risk assessments

**New elements**: (government scheme Cyber Essentials)

* Privacy by design
* Pseudonymisation
* Data minimisation
* Explicit references to encryption

Examples:

1. If you give staff phones work related stuff needs to be protected
2. Make staff anonymous or pseudononymous
3. Stuff on computers should be on a need to know basis only so check limits.
4. Policies should contain guidance on e.g. working off site, locking unattended screens.
5. Staff working at home must be able to work securely by logging into their work desktop and not through their own domain.

Privacy Impact Assessments (**PIA’s**)

There is an obligation to carry out a PIA for high risk activities e.g. introducing a new IT system is deemed high risk or a new piece of software that picks up key words.

A PIA must set out:

* A description of the activity and its purpose
* An assessment of why it is necessary and the right thing to do
* An assessment of the data protection risks
* Measures taken to mitigate the risks.

Example – if the school has a contract with a company to clean up its files and then dispose of old hard drives and subsequently information leaks out from that source the school would be fined because despite having a clause about complying with data protection laws in the contract the school would be deemed not to have done enough to check that they were compliant i.e. the contract is not enough on its own.

**Data Processors**

Schools need a written contract requiring a contractor to keep information secure and must check continuously that they are compliant with data protection law.

The contract must contain clauses that require:

* The data processor to delete or return personal data
* The contractor to provide information about its compliance and allow audits and inspection
* Them to inform the school immediately if the school’s requirements breach the law on data

The contracts you must check for compliance are:

* Pay roll
* Data
* Cloud

If you don’t check you could be held liable.

Drop Box may be an issue because it is American and so comes under different legislation. America has Privacy Shield but it is now being said that this is not sufficient to meet the new regulations. The European commission has produced model wording for contracts. Google is trying to match that and Windows is transferring data to the UK.

**Evidence of Compliance – start now, it is going to be a legal requirement.**

1. **Appoint your Data Protection Officer – this is a mandatory appointment for all public bodies which includes schools** (this person must be independent of Senior management, they can be an employee but can’t be ‘punished’ for anything uncovered)
2. Audit your data, where is it?
3. Who has access?
4. Why are you keeping it?
5. What is it and what is personal data?
6. Who receives it?
7. Is it ever transferred overseas and why?
8. How long do you keep it?
9. What technical and organisational security measures are in place?

**Privacy Notices**

**All schools are required to have a privacy notice –** children can exercise their rights from the age of 12 so the notice must be written in such a way that a 12 year old can understand it.

The notice must contain:

* The identity of the Data controller
* Say what personal data is collected
* State what the personal data is used for
* Say who it is shared with
* It must say that it applies to all staff, pupils, parents, governors, volunteers, etc.
* Information about the right to complain to the ICO
* The legal basis for processing
* How long the data is kept

The notice must be displayed prominently e.g. schools website, employment manual, pupil’s handbook, etc.

The notice is there to inform people not to get consent.

**Subject Access Requests (SAR)**

1. The time period for compliance is to be reduced to 1 month and there is **no** exception for non-school working days.
2. You may not charge for an SAR however you can refuse and/or charge if the request is ‘manifestly unfounded or excessive’.
3. You can ask for the person to specify exactly what they want to see if you have lots of information or you have to go a long way back in time.
4. If the information is wrong people have the right to rectification and restriction of use and where it goes e.g. if you have made a report to Social service which turns out to be inaccurate you must go back and correct it.
5. People have the right to be forgotten so they can request that data be deleted.
6. You do not have to pass on correspondence with solicitors, safeguarding stuff, health matters, or anything which you may feel may harm the child.
7. You must not pass on 3rd party information e.g. if a parent makes a complaint about a member of staff.
8. Emails are subject to the SAR but you do not have to pass on the whole email. You can lift out the information and make a separate document.

**Marketing and fundraising**

The definition of marketing goes beyond selling goods and services.

Consent forms need:

* Transparent so they must include a privacy notice
* There must be consent for any marketing.

Issues could arise from:

* Sharing data with e.g. alumni association
* Wealth analysis and profiling of possible donors
* Historic data
* Use of photographs for publicity
* Fundraising

Solution may lie in:

* Having a tick box letter which tells people how the school uses data and that can act as a record of information given
* Schools don’t necessarily need to get parent’s consent about e.g. photo’s but must tell parents so they can object
* Up to Y6 parents give consent; Y7+ consent needed from pupils and parents. In the 6th Form the students alone can give consent, parents are only legally entitled to the annual report.

For immediate action:

* Audit school’s data flow e.g. what have you got and where is it?
* Look at information security
* Check contracts with data processors
* Review policies and procedures
* Review privacy notices
* Look at risks around fundraising and marketing
* Check for GDPR compliance
* Ensure data systems work to support compliance and include such things as the right to be forgotten and data portability.

**You must have or risk being fined:**

* **An overarching data protection policy**
* **Information security and rules about bringing your own device to work and working at home**
* **An ICT acceptable use policy including Facebook, intellectual property use etc.**

**If it all goes wrong………**

1. **Take immediate steps to contain the problem and sort it out**
2. **There is currently no legal requirement to report the breach but if it is likely to go further it is better to inform the ICO and also for Academies the ESFA**